# PowerShell

PowerShell is Windows new shell. It comes by default from Windows 7. But can be downloaded and installed in earlier versions.

- PowerShell provides access to almost everything an attacker might want.
- It is based on the .NET framework.
- It is basically bash for windows
- The commands are case-insensitive

## Basics

So a command in PowerShell is called **cmdlet**. The cmdlets are created using a verb and a noun. Like `Get-Command`, Get is a verb and Command is a noun. Other verbs can be: remove, set, disable, install, etc.

To get help on how to use a **cmdlet** while in PowerShell, the man-page, you do:

```
Get-Help    <cmdlet    name    |    topic    name>
```

Example

```
get-help echo
get-help get-command
```

Find out what flags you can use just write `get-command -` en then start tabbing.

**Powershell Version and Build**

```
$PSVersionTable
```

### Fundamentals

With get-member you can list all the properties and methods of the object that the command returns.

```
Get-Member
For example:
Get-Command | Get-Member
Get-Process | Get-Member
```

Select-XXX

```
Select-object
```

#### Variables

```
$testVar = "blabla"
```

**Wget / Download a file**

```
Invoke-WebRequest <uri>
wget <uri>
```

**Grep**

```
Select string can be used like grep
get-command | select-string blabla
```

**General commands that can be used on objects**

```
measure-object -words
get-content fil.txt | measure-object words
```

### Working with filesystem

**List all files in current directory**

```
get-childitem
gci

List hidden files too
gci -Force

List all files recurisvely
gci -rec

Count the files
(get-childitem).count
List all files but exclude some folders
gci -exclude AppData | gci -rec -force
```

### Working with files

```
Read a file
Get-Content
    gc
    cat
Count lines of file
(get-content .\file).count
Select specific line in a file (remember that it starts from 0)
(gc .\file.txt)[10]
gc .\file.txt | Select -index 10
```

### Services

```
List services
get-service
```

### Network related stuff

Domain information

```
Get-ADDomain
Get-AdDomainController
Get-AdComputer
To see a list of all properties do this
get-adcomputer ComputerName -prop *

Get AD Users
Get-ADUser -f {Name -eq 'Karl, Martinez'} -properties *

Get all AD Groups
Get-ADGroup -filter *



Resolve DNS
Resolve-DNSname 10.10.10.10
```